CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Conformité et Analyses de Risques

L'analyse des risques au secours de la conformité *(et vice versa)*

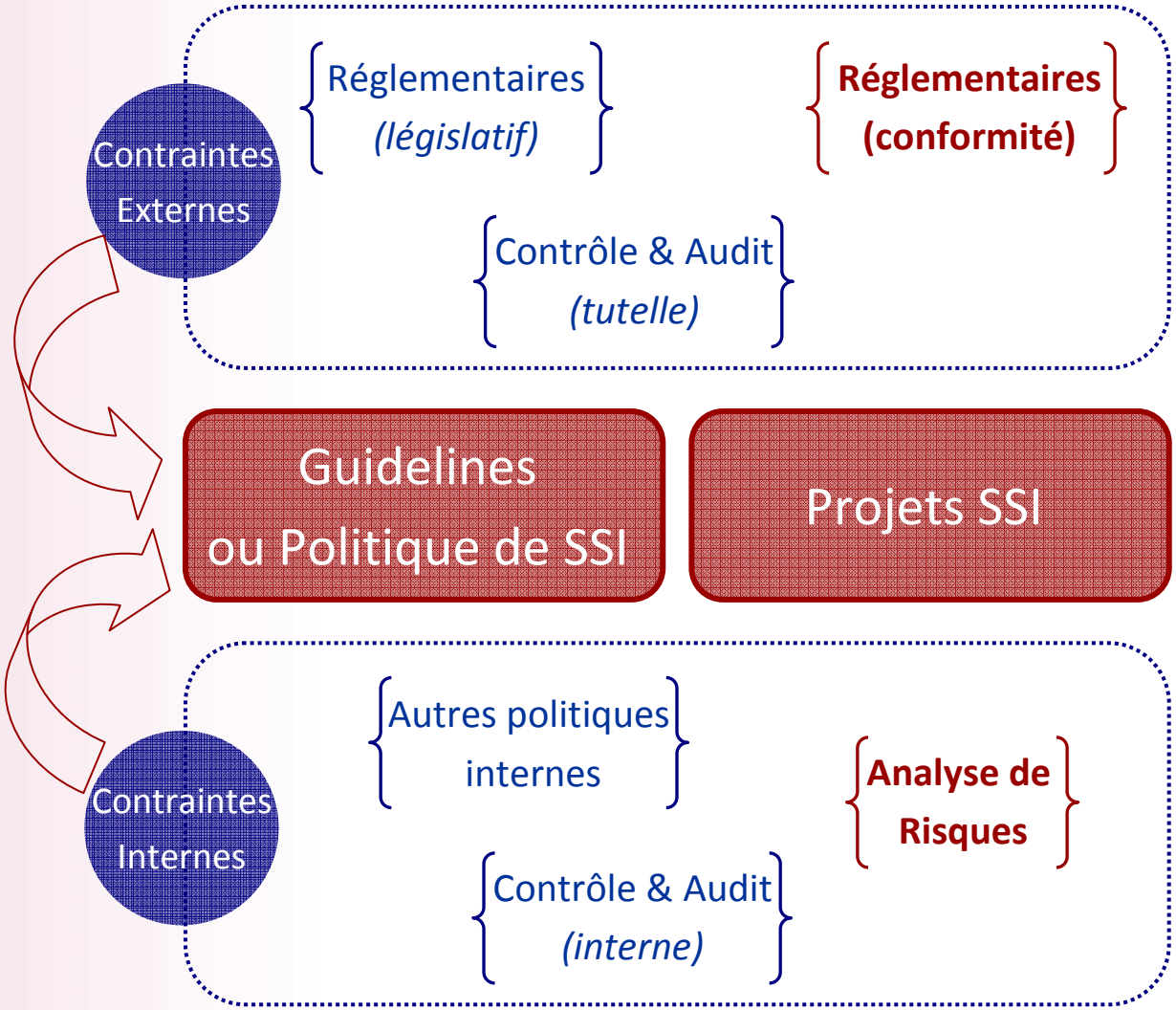
13/12/2012

Baptiste PARENT, Expert Sécurité SI
CNAMTS

CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

De quoi parle t'on ?



Comment proposer une **Gouvernance des risques IT cohérente** *(et plus particulièrement des risques SSI)* en prenant en compte ces différents facteurs.

Diapositive 2

t2 Quelle différence?
tchiofalo; 11/12/2012

REX : Refonte de la PSSI de l'Assurance Maladie

- Construire une nouvelle **politique de sécurité SI globale** pour l'entreprise basée :
  - sur une analyse de risque spécifique visant à couvrir un large spectre de risques :
    - ***métiers,***
    - ***organisationnels,***
    - ***techniques,***
    - ***réglementaires.***
  - sur le besoin de conformité imposé par les autorités de tutelles.

Une démarche assez classique

- Démarche en 3 phases :
  - **Analyse des risques** : identification des risques pesant sur les principaux processus et apprécier les impacts au regard des enjeux de la CNAMTS *(livrable : cartographie des risques)*
  - **Rédaction de la PSSI** : élaborée au regard des risques restant à couvrir identifiés en phase 1 *(livrable : PSSI V4)*
  - **Constitution du plan de traitement des risques** : mise en place des dispositifs opérationnels visant à couvrir les risques identifiés en phase 1 *(livrable : Plan de traitement des risques)*

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Focus sur la méthode d'analyse de risques *(1/2)*

Sources de menace

Référentiel Contrôle Interne

Processus | Processus | Processus

Système d'information

Réseau | Logiciel | Machine

Personne | Canaux de com.

provoquent

Évènements redoutés

Évènement redouté	Source de menace	Impacts	Gravité
Interception ou divulgation d'informations sensibles manipulées par la direction	Négligence ou malveillance d'un agent Malveillance d'une personne externe	Dégradation du climat social interne. Dégradation de l'image de l'Assurance Maladie susceptible de provoquer des débats publics.	Critique

Scénarios de menace

Référentiel EBIOS 2010

Focus sur la méthode d'analyse de risques *(2/2)*

PAR TYPE D'ORGANISMES

Reprise des évènements et des scénarios organisme 1

Reprise des évènements et des scénarios organisme 2

Reprise des évènements et des scénarios organisme 3

1

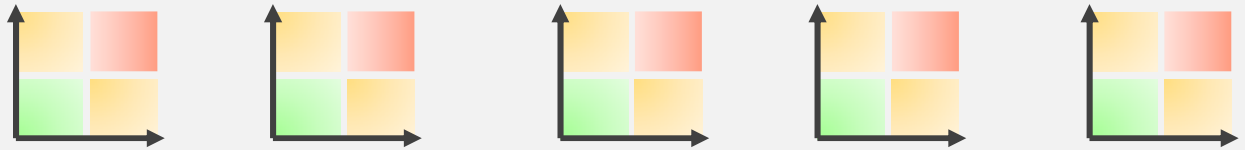
2 Regroupement par processus et nature des risques

Organismes

4 Finalisation

Évaluation des familles de risques par type d'organisme

3

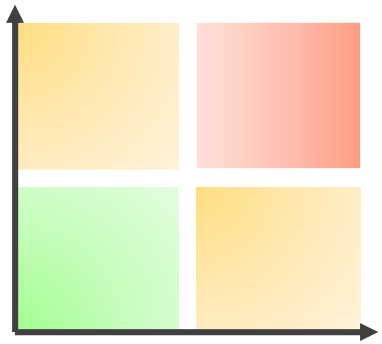


Formalisation des risques et évaluation d'un niveau de risque

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Exploitation des résultats de l'analyse de risques.

Phase de recueil



Cartographie des risques par type d'organismes (CPAM, CTI, CGSS, DRSM, etc)

Fiches de risques

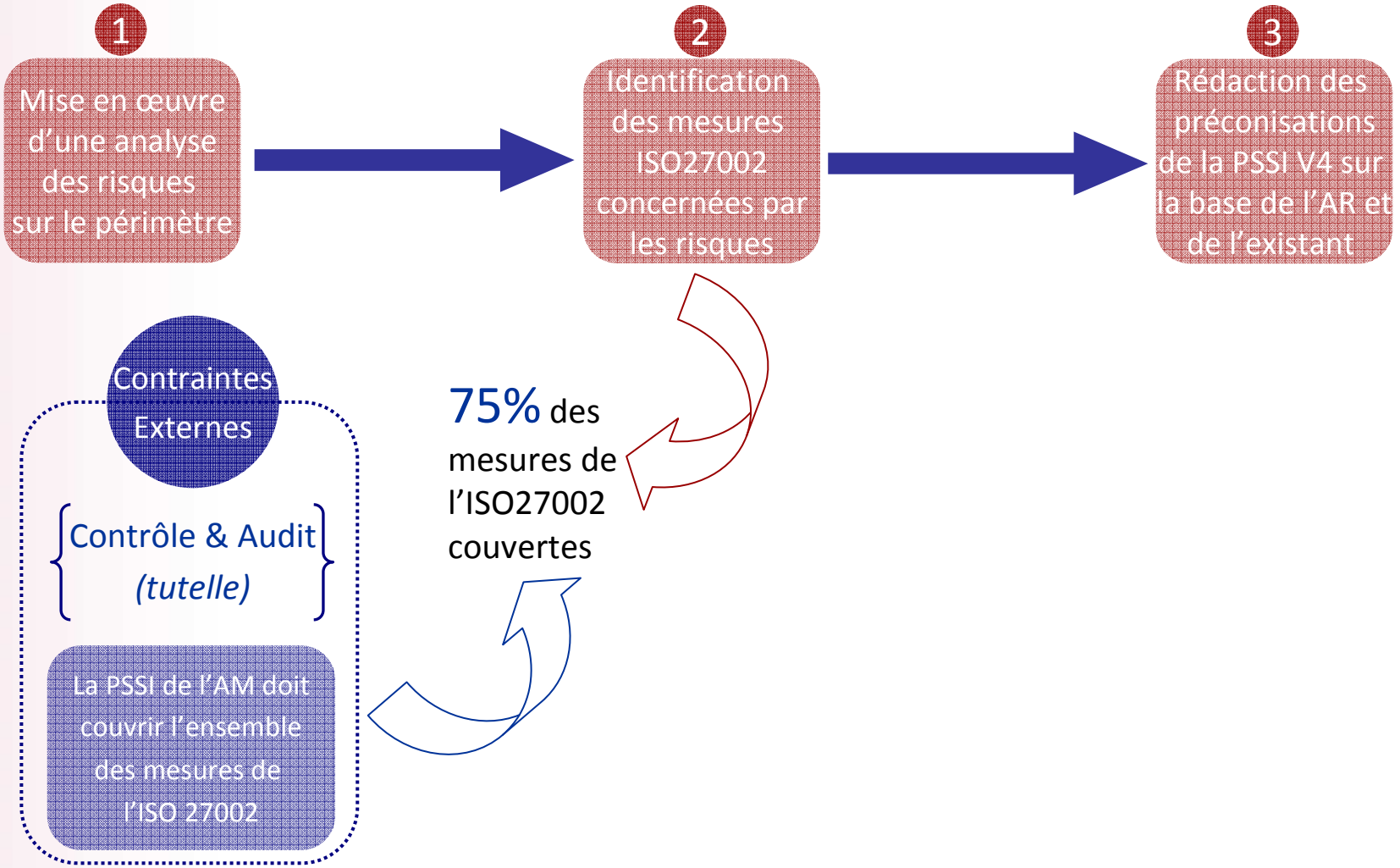
1. Identification des moyens de couverture déjà en place

2. Identification des mesures ISO27002 concernées par les risques (DDA)

Et la prise en compte des besoins de conformité ?

3. Rédaction des préconisations de la PSSI V4 sur la base de l'AR et de l'existant

Notre besoin de conformité imposé par la Tutelle.

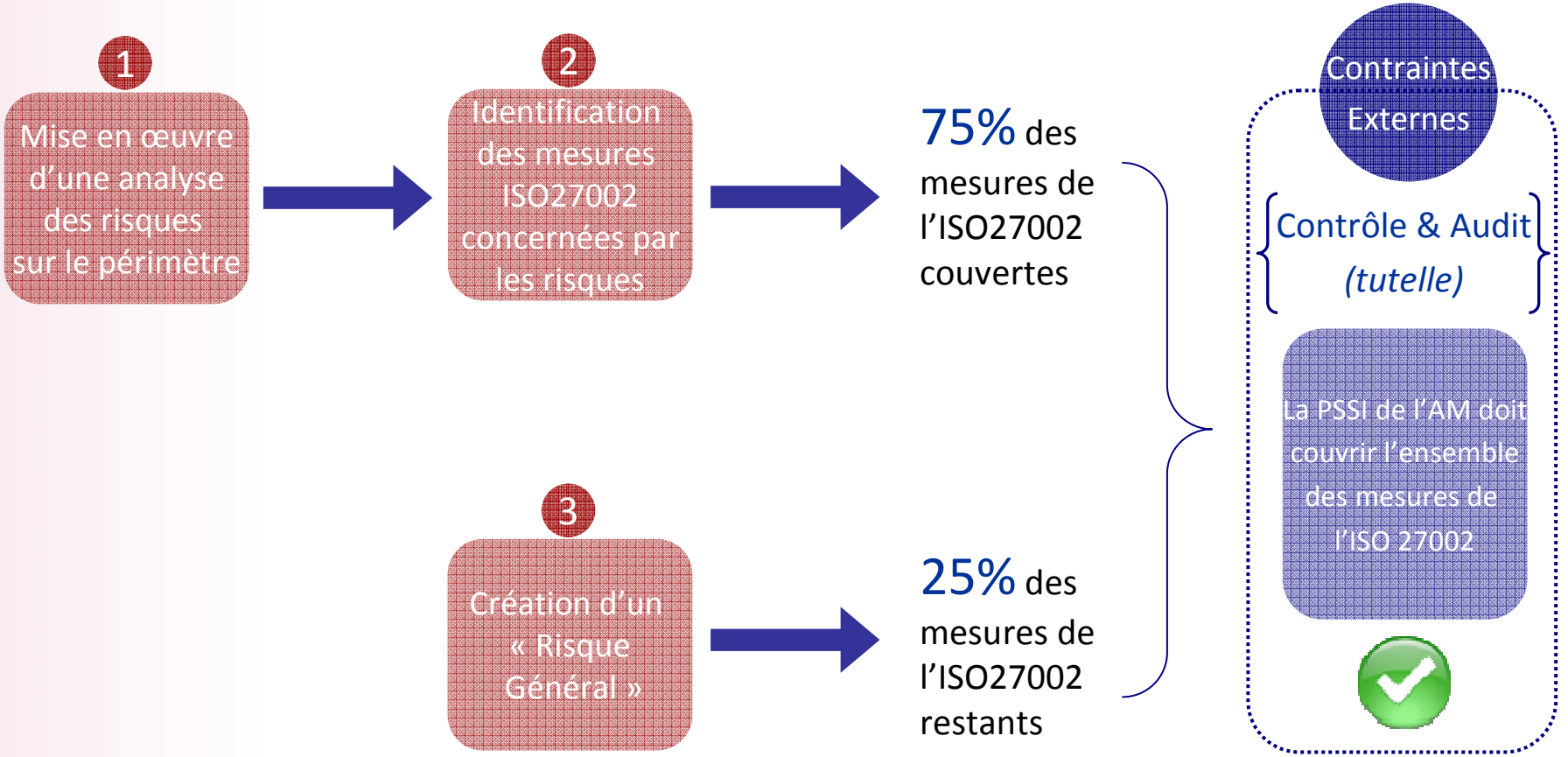


« Analyse de risque » versus « Conformité »

Comment répondre à ce **besoin de conformité** sans trahir les **apports de notre analyse de risques** ?

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

« Liberté » ou « Astuce » méthodologique ?



Une question légitime

Pourquoi faire **une analyse de risques** si l'objectif demeure la **couverture exhaustive de la norme** ?

Une largesse méthodologique peu gênante.

- Malgré un périmètre de couverture qui n'était pas exhaustif, notre « DDA » couvrait néanmoins l'ensemble des chapitres de l'ISO27002.
- Dans ce contexte, la non couverture des 25% restant pouvait avoir pour cause :
  - la **non exposition** au risque concerné par la mesure *(évidemment…),*
  - la **non identification** d'un risque au cours de l'analyse,
  - une **erreur** ou un **oubli** dans le mapping réalisé entre les risques et les mesures ISO 27002.

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Comment préserver l'apport de l'analyse de risques ?

1. Mise en œuvre d'une analyse des risques sur le périmètre

2. Identification des mesures ISO27002 concernées par les risques

\+ 3. Création d'un « Risque Général »

Le travail réalisé au niveau «mesure » permet de viser **l'objectif de conformité** *(par ailleurs, dans un SI classique aujourd'hui il est difficile d'exclure totalement un chapitre de l'ISO 27002)*

4. Rédaction des préconisations de la PSSI V4 sur la base de l'AR et de l'existant

\+ 5. Gestion des Priorités et Plans d'actions

Le travail réalisé au niveau «préconisation» permet de rédiger des consignes qui prennent en compte :
- **l'analyse de risques réalisée**,
- **l'organisation et les mesures existantes.**

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Questions ?